National Aeronautics and Space Administration

COTS EEEE parts: What do the data and experiences tell us?

Jesse Leitner, Chief SMA Engineer, NASA GSFC

Jesse “dot” “Leitner” at “nasa.gov”

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

SAFETY and MISSION ASSURANCE NASA Goddard

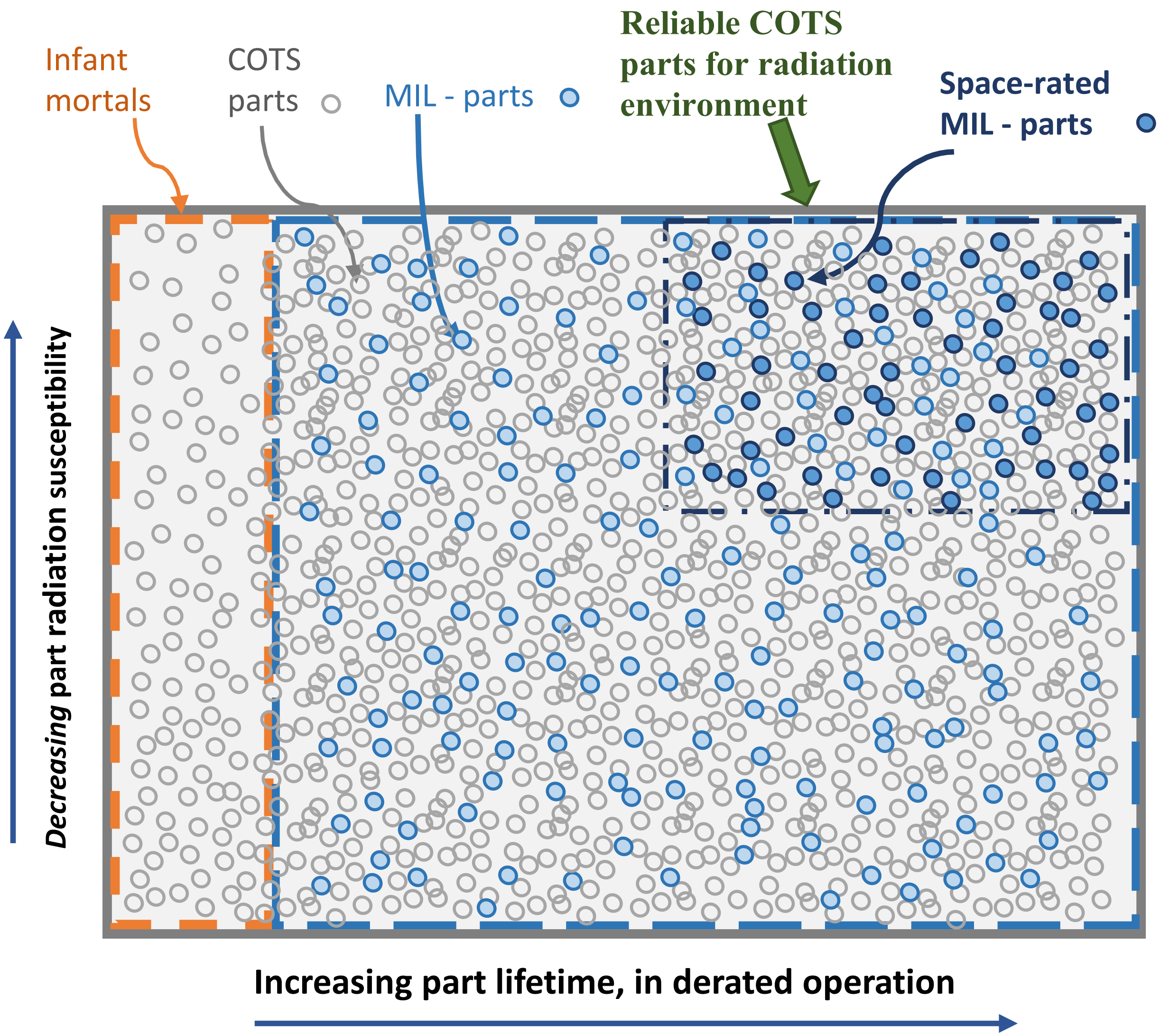
Outline

- Progression of parts assurance in the agency
- COTS EEEE parts in space over time
- Infinite space use of COTS
- Current COTS EEEE parts usage options
- Recent history of COTS EEEE parts in space
- Upscreening of parts – what we learned from Swift
- What do about radiation
- Summary

Progression of Parts Assurance in NASA

- Pre-1995: largely MIL-SPEC (space grade, “Class S”)
- 1995: 311-INST-001 – MIL-SPEC levels 1-3 with upscreening to make up differences in levels
- 2003: EEE-INST-002 – levels 1-3 with upscreening to make up differences and add MIL-SPEC screens to COTS parts + derating
- 2004: NPR 8705.4 guidance – levels 1-3, aligned with classification, or “center parts management plan”
- 2017: NASA-STD-8739.10 introduces level 4 (“grade 4”) – COTS with no additional testing. Declares automotive parts and hi-rel COTS to be level 3 compliant (although not formally implemented in practice in the agency)
- 2021: NPR 8705.4A adds the option for level 4 for Class D
- 2021: SMD Class D MAR: Level 4 baseline for Class D
- 2022: NESC COTS Phase 2 report provides guidance for reliable use of COTS EEEE parts without additional testing, through careful selection

The Infinite "Space" View of COTS



Some recent history of COTS EEEE parts in space

- 2004: Swift mission flies 40% COTS EEEE parts (with level 3 upscreening)
- 2013-2017: Multiple Spacecube variants with up to 99% COTS EEEE parts (no upscreening)
- Numerous Ames missions, 100% COTS EEEE parts (no upscreening)
- Ingenuity: 99% COTS EEEE parts with focused screening
- SpaceX: Mostly COTS EEEE parts
- SSTL: Mostly COTS EEEE parts(several decades)
- AFRL's Ascent: 100% COTS EEEE parts (GEO)
- Newspace: almost 100% COTS EEEE parts and components

SpaceCube Time-on-orbit

As of Oct 2021 (STP-H6 was turned off Dec 9, 2021 to make room for the next instrument)

Project	Version	Part Req	BOM Count	Operation Months	Xilinx Quantity	COTS %	COTS Months
RNS	v1.0	2+	3700	0.0833333	4	1%	3.08333
MISSE-7	v1.0	N/A	3100	90	4	2%	5580
SMART	v1.5	N/A	1000	0.0333333	1	95%	31.6667
STP-H4 CIB	v1.0	N/A	1500	30	2	1%	450
STP-H4 ISE2.0	v2.0-EM	N/A	1250	30	3	98%	36750
STP-H5 CIB	v1.0	N/A	1500	46.933333	2	1%	704
STP-H5 ISEM	v2.0 Mini	N/A	1000	46.933333	1	26%	12202.7
STP-H5 Raven	v2.0-EM	N/A	1500	46.933333	3	99%	69696
RRM3	v2.0	N/A	1429	36.666667	2	65%	34057.8
STP-H6 CIB	v1.0	N/A	1500	31.833333	2	1%	477.5
STP-H6 GPS	v2.0	N/A	1157	31.833333	2	65%	23940.3
Restore-L Lidar	v2.0	3	2000		2	0%	N/A
STPSat6	v2.0 Mini	N/A	1500		1	98%	N/A

Totals	Units Flown	11
	Commercial FPGAs	26
	Commercial FPGA Device-Years	83
	Part Years	57213
	COTS Parts Years	15324

Also to note: We flew many COTS components on some of these projects:

- ISE2.0, SMART, and ISEM all flew COTS cameras that were ruggedized. SMART flew COTS SATA drives.
- Raven flew a $5 USB interface card to an IR sensor
- STP-H5 and -H6 have CHREC Space Processors (CSPs) that were 95% COTS components. See references for more info on CSP results (no failures to date)
- RRM3 suffered a failure (outside of SpaceCube) that may have involved a specific COTS part, but the part was used in a stressing condition that any part would eventually fail.
- NavCube Commercial vendor populated PWBs

About MIL-SPEC "upscreening" of COTS parts – what did Swift tell us?

- Why would it ever make sense to apply a 30-50-year-old test to a recently designed and manufactured component?
- Can you make a poorly-selected part high quality or high reliability by applying tests to it?
- Why did we not learn this lesson from Swift (2004)? Can we learn it today, 18 years later?
  - "SWIFT BAT parts engineering successfully executed a parts control and test program that assured that all parts met or exceeded Grade 3 [sic] program requirements, including radiation tolerance. There were a few scattered failures during parts testing, but the subsequent failure analyses revealed that the failures were due to mishandling or improper testing at the board or box level."
  - But yet, "Design engineers elected to select plastic parts, which allowed the use of state-of-the-art devices that provided the advantages of lower power, volume, and weight. However, commercial-grade parts are designed for a very different set of operating conditions than those found in a space application. A full and thorough evaluation is needed for any part type proposed for space flight use like the ones used on the SWIFT BAT project." ---- is this really the lesson we should have learned?

Broad sweeping statements are used even when context is available

What should be done about radiation?

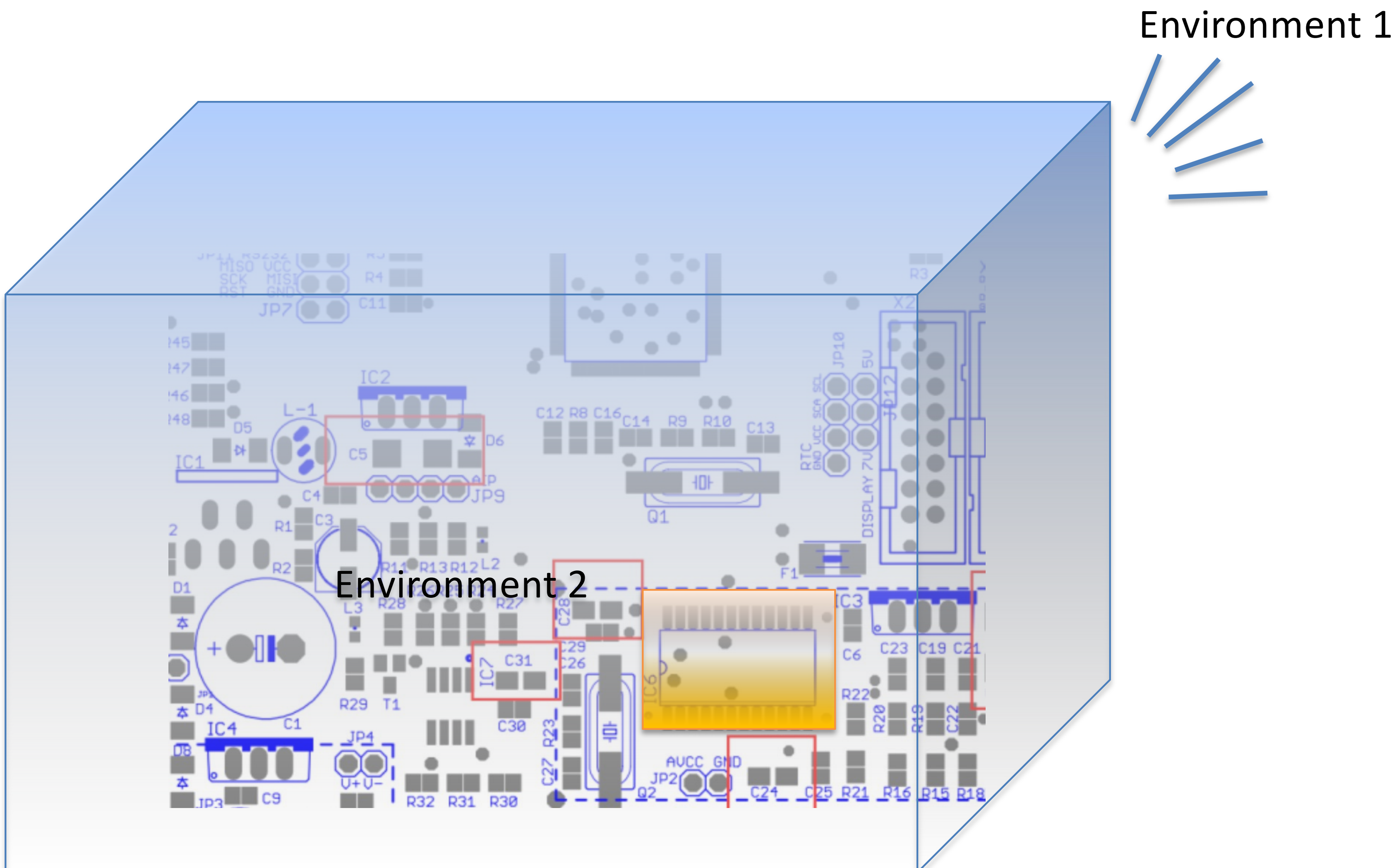
- Using new parts and new technologies will demand a new approach for radiation
- Any expectation that all or most parts will be rad-hard or tested for radiation from their current lots will simply cause many to collapse under their own weight (including many that have been in space successfully for decades)
- Any expectation that radhard parts are necessary and sufficient for successful on-orbit operation will lead to disappointment (as in SMAP)
- Use good system design practices – transition from rad-hard parts to *rad-hard assurance by design*
  - Radiation hardness/susceptibility determined at the circuit/system level, not at the part level
  - Similar to many references in literature to “rad hard by design” (RHBD) as opposed to “rad hard by process” (RHBP, hardness of individual parts)
  - Mission, Environment, Application, and Lifetime (MEAL) are defined in the circuit, not outside of the spacecraft (parts are not seeing the environment outside of the spacecraft unless they are outside of the spacecraft with limited circuit influence).
  - Latchup-susceptible parts should be protected by redundancy or latchup protection circuits*
- Use familiar parts
  - New sensitive part types (CMOS, processors, MOSFETs, memory, LEDs etc) in critical applications should invoke testing or sufficient protection, which should be a strategic element of PEAL, not inline with projects
- Use higher-level components and assemblies that have flown in similar environments
- **Learn from on-orbit experiences as the primary means for radiation assurance.**

*See, e.g., J. B. Carlsen, “Design and Validation of Two Single Event Latch-up Protection Solutions”

How do we define MEAL for a EEEE part?

- Is the environment outside of the spacecraft?
- How does the application come into play?
- Does the application include the circuit design?

Which represents MEAL?



Application

- Which has greater reliability?
  - a space-proven non-RHA part using TMR
  - An RHA part without TMR
- Which has greater reliability?
  - One RHA MOSFET with 40 nm gate oxide in an SMD-2 package
  - Three non-RHA MOSFETs with 5 nm gate oxide in DPAK

P/N	IRHNA57160	STD100N10F7
VDSS	100V	100V
ID	75A	80A
RDS(on)	12 mΩ	8 mΩ
Package	SMD-2 (~232 mm^2)	DPAK (~60 mm^2)
Weight	3.3 g	0.33 g

Summary

- COTS EEEE parts have been flying in space extensively for years with great success
- There is no known failure history of COTS parts that have been properly used, with proper system design and test
- Opportunities to learn from COTS experiences have been skewed by broad statements rather than facts and analysis
- The approach for solving the radiation problem at the piece part level has put up an additional barrier against COTS, without actual evidence to support
- In order to move forward, a fresh look at what makes parts reliable in usage is required

How are automotive and hi-rel COTS defined?

- Declared by the manufacturer to be intended for reliable usage
- Characterized by extensive in-production and/or post-production screening or electrical testing as evidenced by one or more of the following
  - Description in the datasheet
  - Manufacturer-provided documentation, such as
    - Production Part Approval Process (PPAP) document
    - Quality Manual
    - Website detailed technical information provided
  - Parts are qualified to the pertinent AEC Q-category specification (Q100, Q101, Q200)
  - Production is managed under IATF 16949 quality management system (QMS)

Current options for use of COTS EEEE parts in the agency

- Class D and sub-Class D: no restrictions at the agency level, COTS EEEE parts are recommended. Smart selection and use of COTS is always encouraged
  - Known parts from reputable manufacturers, sold for reliable use
  - Respect the datasheet
- Class C (level 3): Automotive and manufacturer hi-rel COTS EEEE parts are compliant as-is IAW NASA-STD-8739.10. Language being incorporated into GSFC SMA MAR templates for Class C.
- All Classes: Standard components that include internal COTS EEEE parts accepted based on history of the item relative to the current environment (part selection and assurance delegated to standard component manufacturer)
- All Classes: Pilot implementation of “three-option” part assurance

NESC COTS study

- Originally formed to support the Commercial Crew Program and its heavy use of COTS
- Turned to focus on the overall problem of selection, evaluation, screening, qualification, and usage in robotic and human-rated space systems
- Phase 1 introduced several new ways of looking at COTS and key terminologies to help the agency understand ways to use COTS successfully
- Phase 2 has extensively dispelled myths and established a framework for new approaches to use COTS parts reliably
  - Reliable usage centers around the concept introduced in the Phase 1 study, the Industry Leading Parts Manufacturer (ILPM), and the specific selection of Established parts

This presentation was largely motivated and informed by the NESC COTS study, but it goes well beyond the findings and message of the study

ILPM

ILPM: a COTS manufacturer that produces high quality and reliability parts that do not require additional screening and lot conformance testing, common in today's requirements for using "non-standard" parts in space

- Implements a "Zero Defects" program, as described in AEC-Q004 or a similar source.
- Designs parts for manufacturability, testability, operating life and fielded reliability.
- Manufactures parts on automated, high-volume production lines with minimal human touch labor.
- The manufacturer understands and documents all manufacturing and testing processes and the impacts and sensitivities of each process step on product characteristics and quality.
- The manufacturer's end-product testing includes 100% electrical verification of datasheet parameters.
- The manufacturer implements rules for removing outlier parts and removing abnormal lots; these rules may apply either in-process or with finished parts.
- The manufacturer implements a robust change system that assures all major changes are properly qualified and that customers are notified of major changes
- The manufacturer implements a robust Quality Management System acceptable for spaceflight.

Each organization should maintain its own list of ILPMs

Established Part

- Produced using processes that have been stable for at least one year so there are enough data to verify the part's reliability;
- Produced in high volume. High volume is defined as a series of parts sharing the same datasheet having a combined sales volume over one million parts during the part's lifetime;
- 100% electrically tested per datasheet specifications, minimally at typical operating conditions and is in production prior to shipping to customers. Additionally, the manufacturer must have completed multi-lot characterization over all operating conditions cited in the part's datasheet, prior to mass production release. Thus, production test limits are set for typical test conditions sufficient to guarantee that the parts will meet all parameters' performance specifications on the datasheet;
- Produced on fully automated production lines utilizing statistical process controls (SPC), and undergoes in-process testing, including wafer probing for microcircuits and semiconductors, and other means as appropriate for other products, e.g., passive parts. These controls and tests are intended to detect out of control processes and eliminate defective parts at various stages of production.

COTS parts

- Parts designed for commercial applications for which the part manufacturer solely establishes and controls the specifications for performance, configuration and reliability, including design, materials, processes, and testing without additional requirements imposed by users and external organizations. It is typically available for sale through commercial distributors to the public with little or no lead time.
- Manufacturers design for reliability and employ continuous improvement processes and advanced manufacturing techniques
- Manufacturers perform their own qualification tests based on how the parts are manufactured and how they are intended to be used
- Reliability is established by volume
  - Reliability is essential to stay in business, so it is self-controlled and *stable*
  - Low volume parts have questionable and uncertain reliability, and thus must be assured by additional means
- Vendor screening and testing processes assure uniformity and that each part performs as intended, while avoiding damaging or degrading parts through additional handling, use of unknown test equipment, and overtesting
  - Parts not going through vendor screening and testing processes have uncertain linkage back to the historical usage needed to form a basis for reliability
- **High-volume parts from reputable vendors that go through 100% vendor screening covering all datasheet parameters have the best opportunity for reliable usage, when used well within rated limits (<u>including radiation*</u>) because testing is most closely linked to actual manufacture and usage.**

*Radiation is a system-level phenomenon that is not sufficiently addressed at the piece-part level

MIL-SPEC parts

- Originated in DoD out of the need for tight uniformity and interchangeability of parts across the world
- Quality specifications were defined to cover the most extreme range of conditions
- The government controls the drawings, requirements, and specifications of such parts.
- Reliability is often declared based on accelerated testing combined with many stringent requirements and other forms of extreme tests
- Some specs/requirements included based on past lessons learned or past indicators of infant mortality
- Originally, MIL-SPECs were the only reasonable approach to procure parts that were necessary to function reliably.
- Thus MIL-SPECs were the best existing source to obtain parts to use in space systems
  - The government monitored parts manufacturing and testing
  - Failure rates from highly-accelerated tests were used to predict reliability and verify that issues were not appearing in manufacturing.
- **MIL-SPEC parts arbitrarily link to reliability because they are assured by quality specifications that may not represent actual usage or manufacture, and may overtest parts by using standard screening practices. Since reliability is a by-product, it is far from guaranteed***

*many MIL-SPEC parts go through extended reliability testing but the testing is not relevant to the actual usage and it does not address the types of failures typically encountered with MIL-SPEC parts

NASA-screened COTS parts

- COTS parts that are screened and/or qualified (level 1 or 2) using MIL-HDBKs via a document such as EEE-INST-002.
- Reliability is equivalent to that of COTS parts except that MIL-SPEC tests are applied to the parts, resulting in frequent overtesting relative to the part application and often to its datasheet. Thus this option provides the greatest uncertainty for reliability, especially if the COTS parts are low volume or low quality to start with.

What are the key drivers for using COTS?
(Not necessarily all at once)

- The need to employ technologies from the past 15 years
- The need for parts that are available
- The need for parts that are affordable
- The need for parts that are the most reliable
- The need for parts that meet mission requirements

Why have COTS been perpetually deemed “unreliable” or “low-grade”

- The COTS definition is infinite
  - This is exacerbated by an infinite number of definitions
    - COTS is often a “label” used at a manufacturer with a local definition
  - “Reliability” defined by the worst elements in the broad category
- MIL-HDBK-217
  - Arbitrary “failure rates” (PEMs 60-600x MIL-SPEC without any current foundation)
  - Approach (along with similar handbooks) has become engrained across the traditional aerospace contractor community
  - Standard “probability of success” (Ps) requirements have demanded its use
- Issues with the plastic used in PEMs in the 70’s and 80’s.
  - Took time to work through challenges to get the materials and manufacturing right
  - e.g. moisture in the plastics were interacting with aluminum, resulting in corrosion
  - Problem was solved in the late 80’s and PEMs ultimately surpassed hermetic ceramics in part-level reliability (failure rates)
- Myths about COTS vs radiation

Why have COTS been perpetually deemed "unreliable" or "low-grade" (cont'd)

- There was a semi-conscious decision dating back to the 70's that all electronic parts flying in space must be rad-hard (by some definition),
  - radiation problem is best solved at the part level,
  - experiences in developing Skylab that concluded that given the immature manufacturing processes at the time it was much better to maximize part assurance practices at the time of manufacture then to add processes later or catch problems in testing.
- Class S part was born
  - Over time, "Class S" became conflated with other MIL-SPEC classifications and radiation hardness was subsequently conflated into the mix,
    - Trapped the community into the mantra that only "Class S" parts can be flown in space; anything else would be a disaster.
    - Had the unfortunate additional consequence that if a failure of a "Class S" part occurred, it was clear that all had been done, and there was no need to take things any farther to challenge whether part of the "Class S" mantra had contributed to the problem.
  - A "Class S vs COTS" notion would perpetuate. In parallel, commercial manufacturing processes were improving and far surpassing this MIL-STD-based control system, which was frozen in time at its inception and unaffected by commercial markets or improving technologies.

Reliable COTS

- Verify part meets Mission Environment, Application, and Lifetime requirements
  - Radiation verified at the part level (RHA in the datasheet is one approach)*, circuit level (circuit design, fault tolerance, circuit protections), or system level (shielding, fault tolerance)
- Use parts from an ILPM
- Use Established parts
- Recognize contexts for risk
- Respect the datasheet (processing, testing, and usage)
  - Do not screen parts outside of datasheet levels
- Do not repeat manufacturer tests
- Low field failure rate or DPPM
- Relationship with manufacturer for transparency and trust

*radiation hardness or tolerance of individual parts is not sufficient for performance in severe radiation environments, as evident from SMAP

Context for Risk in Parts

COTS

- Parts with special features that are difficult to manufacture consistently (never available on MIL-SPEC)
  - e.g., extra-low ESR and ESL ceramic capacitors
- Parts used in brutal operating regimes
  - High-voltage (particularly > 3 kV)
  - Cryo
- Low volume and hand-produced parts
  - Lack a basis for reliability and often do not have optimized manufacturing processes
- Parts used in extremely sensitive (poor) designs (based on variability of parameters not in part spec)
- Parts used in applications in which the environment is unknown
- Parts from unknown or poor-performing vendors (no recent examples)
- No "hi-rel" or automotive parts available

MIL-SPEC

- **All risk-contexts for COTS, plus:**
- Low-volume parts
- Lead time and costs can reduce system-testing resources
- Designed for old manufacturing processes and broad environments
- When used broadly, they can bring false hope and extensive problems may ensue
- Processes will miss new manufacturing flaws
- Performance and reliability not driven by the need to stay in business
- Performance limitations may lead to weak designs

NASA-screened COTS

- **All risk-contexts for COTS, plus:**
- Parts are often overtested since MIL-SPEC testing regimes are not related to actual usage and parts are often not designed or optimized for such regimes
- False hope that screening is relevant to operation
- False hope that screening, testing, and qualification increase reliability or quality
- The prospect for burying a problem or reduced lifetime into a part by the "overtest by design".

Note that the contexts for risk in COTS parts all arise from mission performance requirements that would be present no matter which parts approach is used, so they apply to all cases.

Current Conflicts

- MIL-SPECs, by definition, fundamentally limit technology
  - The broad environmental ranges required and the ability to tolerate many forms of overtest (inherently a derating), drive firm “catalog limits”, which have been in place since inception
  - There are not and will not be well-defined “parts categories” to cover many new classes of electronics technology
- The use of MIL-SPECs to accept and qualify COTS parts conflicts with many of the premises of COTS parts
  - MIL-SPECs involve many test levels that are not based on the actual manufacturing processes or application use of the parts
  - COTS parts are optimized to levels laid out in their data sheets, which would very often be different from MIL-SPEC testing levels (neither necessary or sufficient for properly characterizing the parts for acceptance)
    - MIL-SPEC testing levels can overtest COTS parts, resulting in misleading data and/or reduced reliability and damage to parts

Soon there will be no choice

- Instruments are appearing for high end missions that cannot be manufactured with MIL-SPEC parts or parts that can be effectively screened into compliance using EEE-INST-002
  - It is a virtual certainty this will be the case for the next major flagship space telescope
- Fully COTS spacecraft are soon to be ubiquitous and over time, some will stand out as long-term reliable
  - As long as we continue to equate EEE-INST-002 screening and qualification with reliability, we will continue to misrepresent reliable systems based on COTS as “unreliable”.
  - Such spacecraft will always be frowned upon for usage within NASA
- Availability of MIL-SPEC parts, especially level 1 and many types of space-grade, is becoming a growing challenge, in addition to the growing excessive costs.

Quality and Reliability

- Quality is the totality of features and characteristics of a product or service that bear on its ability to satisfy given needs.
  - In many cases quality is defined by specifications that do not actually link to performance
  - In some cases, such specifications are egregiously more stringent than the application warrants
    - We can coin this term *misguided quality* when the second half of the quality definition is missing
- The reliability of a system is its ability to perform (or the probability to successfully perform) the necessary functions within expected life cycle exposure conditions for a required period
  - Reliability of a system is established through
    - A design that has minimal sensitivity to normal disturbances on the system
    - Established past history of the same product
      - Similar products may be used as a basis but the translation to the current product may be complex
  - We often do not have access to design details for many products, which leads to reliance on
    - Knowledge of the developer's capability to develop reliable products
    - Use of a proven design and tight control of variability

    to establish the reliability basis or claim
- Sometimes the original definition for quality of a given commodity or product is no longer meaningful
  - Technology and manufacturing have changed
  - Evolution of the product design has surpassed the quality definitions
- In many cases, manufacturers use the term *reliability* to represent *quality*
  - This is a practice that is based on past MIL-SPEC definitions.
  - Often the quality definition for a product loses its meaning over time (due to, e.g., manufacturing changes)

Misguided quality

- Imposing stringent and excessive numbers of requirements relative to what is needed to achieve required performance and reliability
- Blindly enforcing extensive requirements on manufactured hardware without considering effects of existing assembly vs that of rework
- Using flight and/or qualification unit testing requirements that greatly exceed mission requirements, thus providing misleading results or overstressing or reducing the life of flight hardware
- Misapplying stringent, but proven, requirements or tests to application areas outside of their original intent and design

Risk Mitigation vs Risk Avoidance

- Risk mitigation
  - Understand actual risks associated with the parts used, COTS or MIL-SPEC
  - Understand and control, when necessary, the risk factors associated with COTS
  - Assure usage of COTS is consistent with their manufacture and datasheet restrictions
- Risk avoidance
  - Ban the use of anything that may involve risk in some scenario, rather than when there is a context for risk in the current scenario
  - Do not perform the function if it requires COTS because COTS are unfamiliar and require a different approach.
  - Using MIL-SPEC parts when established COTS are better fits does not avoid risk; it just converts a fear to a design-based risk.

National Aeronautics and Space Administration

Example COTS space experiences

The SpaceCube

SAFETY and MISSION ASSURANCE DIRECTORATE Code 300

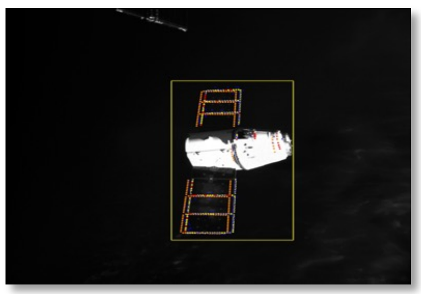
www.nasa.gov

Example: Raven Payload

Objective:

To advance the state-of-the-art in rendezvous and proximity operations (RPO) hardware and software by:

- Providing an orbital testbed for servicing-related relative navigation algorithms and software
- Demonstrating relative navigation to several visiting vehicles:
  - Progress
  - Soyuz
  - Cygnus
  - HTV
  - Dragon

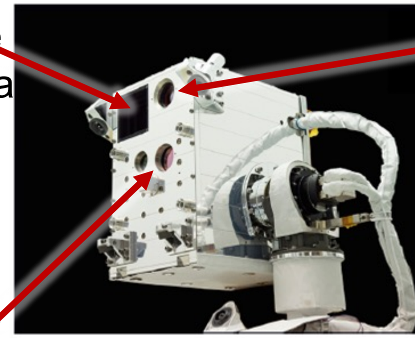


- Demonstrating that both cooperative and non-cooperative rendezvous can be accomplished with a single similar sensor suite

Visible Camera

Infrared Camera

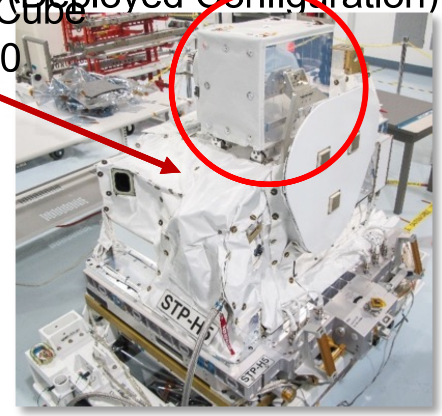
LIDAR



Raven
(Deployed Configuration)

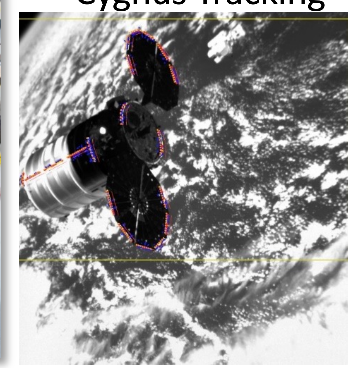
$20M+ payload reliant on confidence in the SpaceCube computer, which in this case was pre-populated with 99% COTS Parts, and then thoroughly tested.

SpaceCube v2.0



Raven installed on STP-H5
(Stowed Configuration)

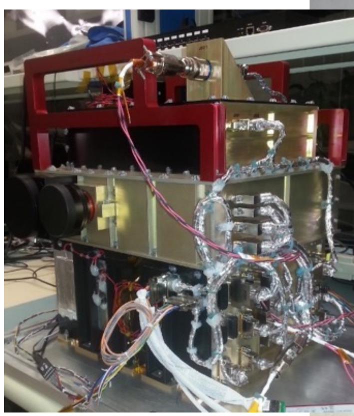
Cygnus Tracking

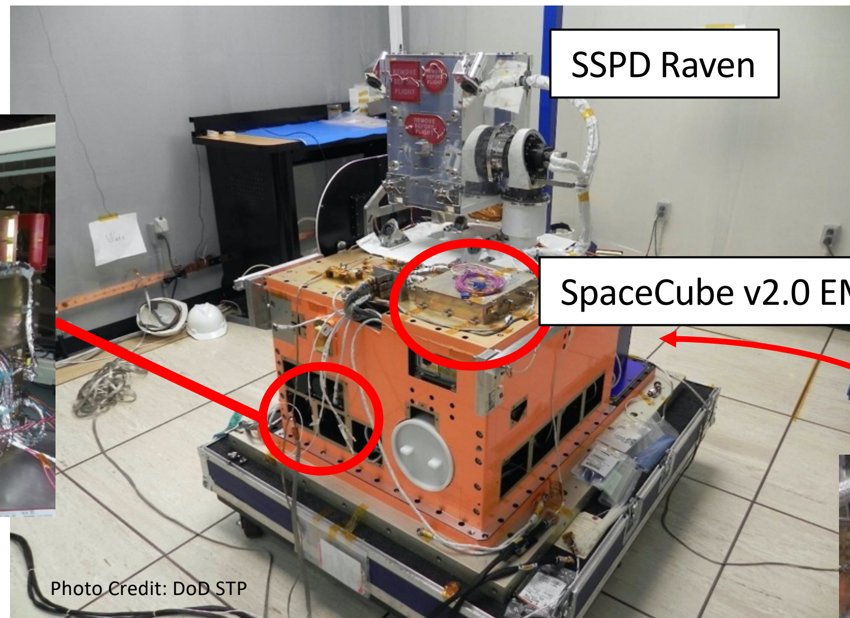


Example: STP-H5 ISS Payload

26% COTS Parts

ISEM, SpaceCube Mini





99% COTS Parts

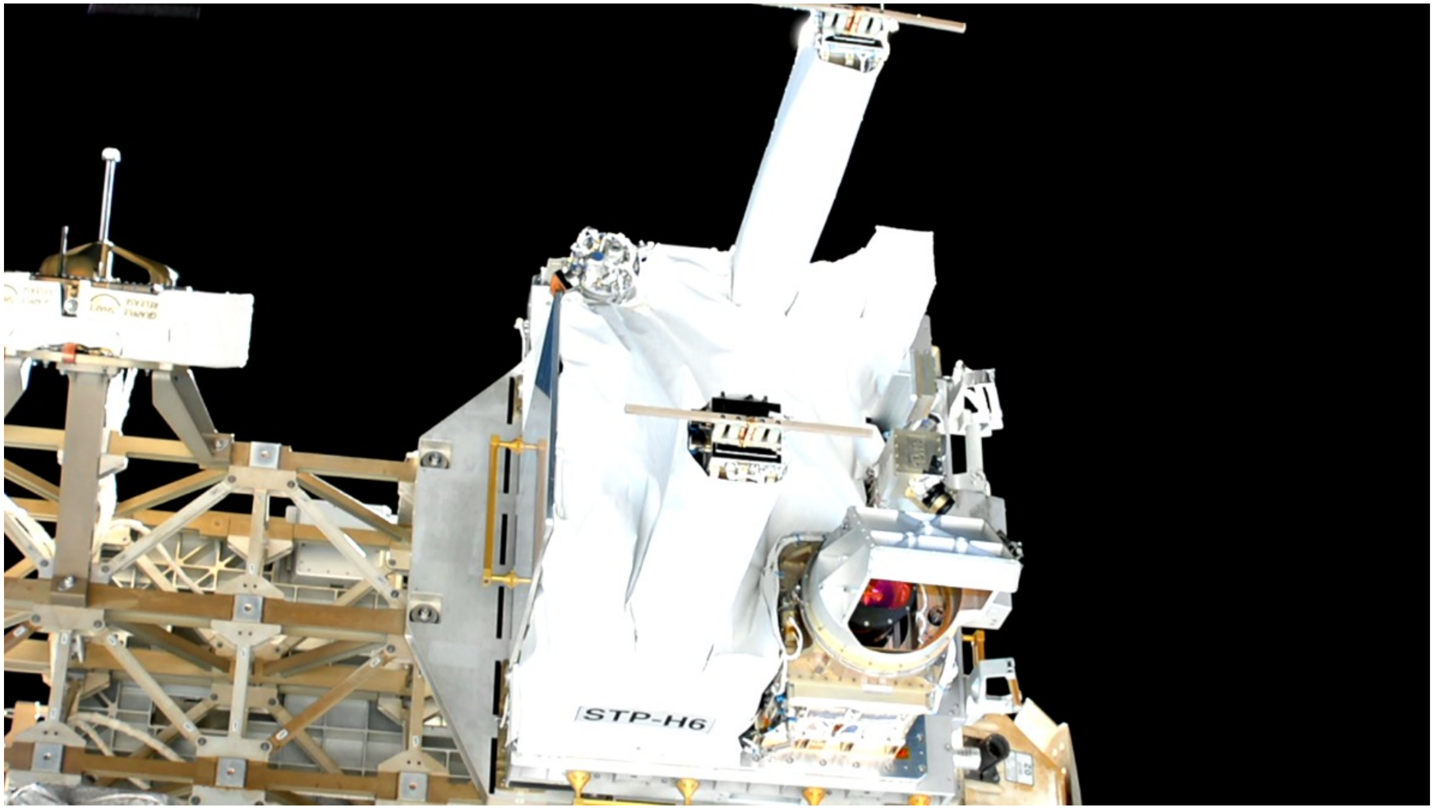
SpaceCube v1.0 CIB

1% COTS Parts

The Space Test Program-H5 (STP-H5) external payload, a complement of 13 unique experiments from seven government agencies, is integrated and flown under the management and direction of the Department of Defense's Space Test Program.

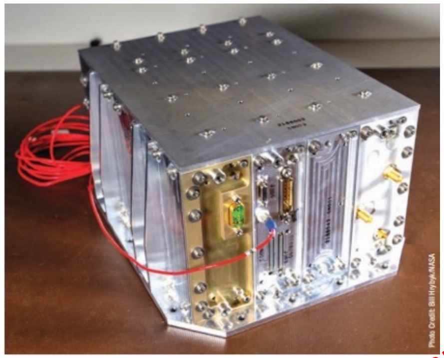
2/2017 - Current

Example: STP-H6 Payload



99% COTS Parts

SpaceCube v2.0 NavCube



1% COTS Parts

SpaceCube v1.0 CIB

Side-by-Side Comparison – Proper use of COTS

Platform:
- SpaceCube v1.0

Parts:
- Level 1 and Level 2 Parts

Application:
- Relative Navigation System
- Hubble Space Telescope Real-Time Tracking using 3x visual cameras

Identical Rigorous Design and Test Philosophy

Platform:
- SpaceCube v2.0

Parts:
- Commercially screened Parts (i.e. COTS)
- Ability to use any level of parts

Application:
- Raven Relative Proximity Ops
- ISS visiting vehicle real-time tracking using visual, Lidar, and IR instruments